PATECCO
dynamic identity systems.

THE 6 PILLARS OF A PRACTICAL INCIDENT RESPONSE (IR) PLAN

By PATECCO

PREPARATION

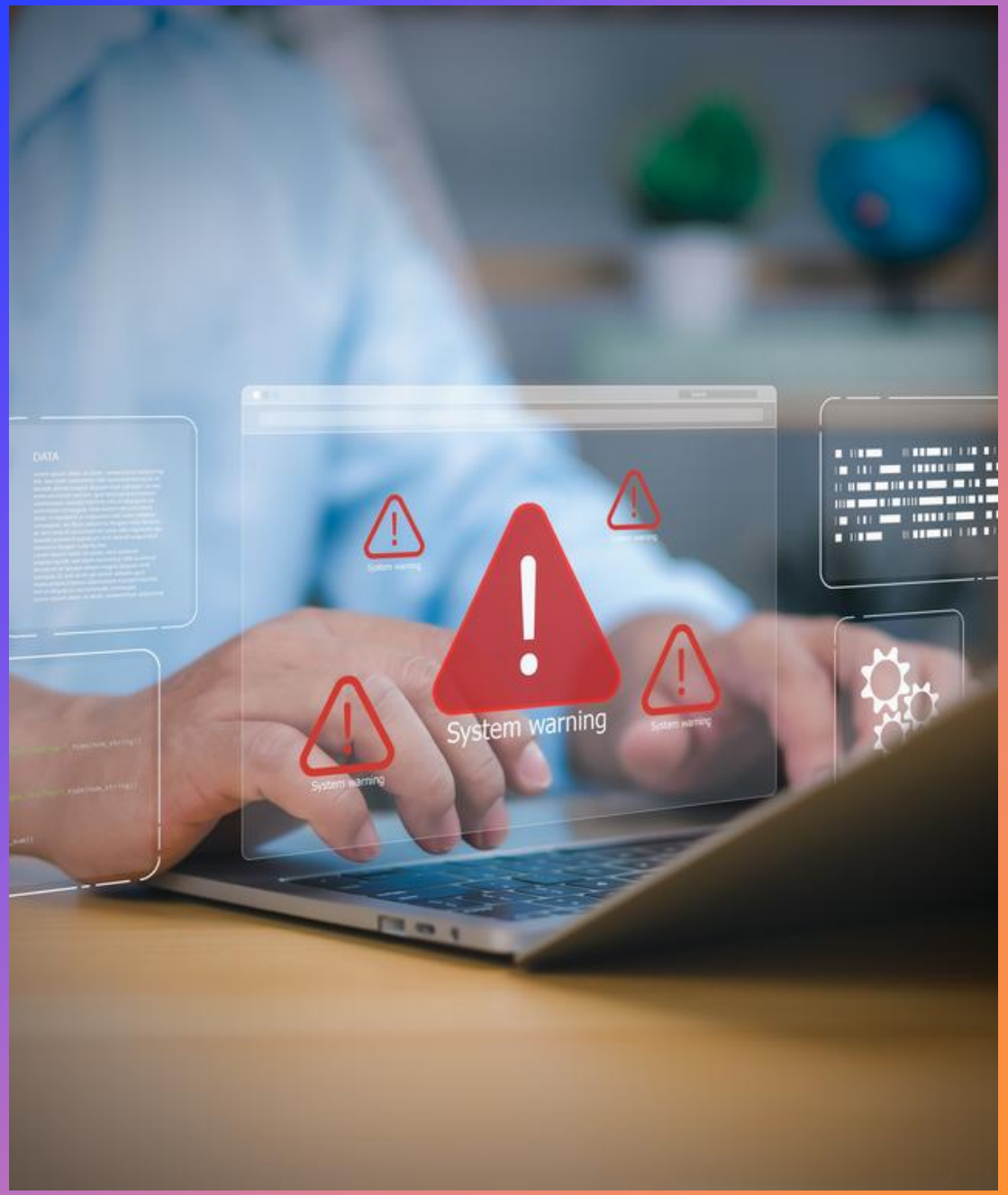
Build the foundation before an incident occurs.

- ✓ Define IR scope, roles, and escalation paths.
- ✓ Maintain up-to-date contact lists (internal + external).
- ✓ Align with regulatory and insurance requirements (GDPR, NIS2).
- ✓ Verify critical backups and monitoring tools are functional.

IDENTIFICATION

Detect and confirm an incident quickly and accurately.

- ✓ Define what constitutes a “security incident.”
- ✓ Use SIEM, Endpoint Detection and Response, and monitoring to capture alerts.
- ✓ Train employees to recognize suspicious behavior and report it.
- ✓ Escalate to IR lead or SOC within minutes, not hours.



CONTROL

Stop the attack from spreading and limit damage.

- ✓ Isolate affected systems or networks immediately.
- ✓ Disable compromised accounts or credentials.
- ✓ Block malicious IPs, domains, or ports.
- ✓ Preserve logs and forensic evidence before cleaning systems.

ELIMINATION

Remove the threat completely and close exploited gaps.

- ✓ Identify root cause and attack vector.
- ✓ Eliminate malware, unauthorized users, or malicious code.
- ✓ Patch vulnerabilities and strengthen configurations.
- ✓ Reset all affected passwords and keys.
- ✓ Update signatures, rules, and detection systems

RECOVERY

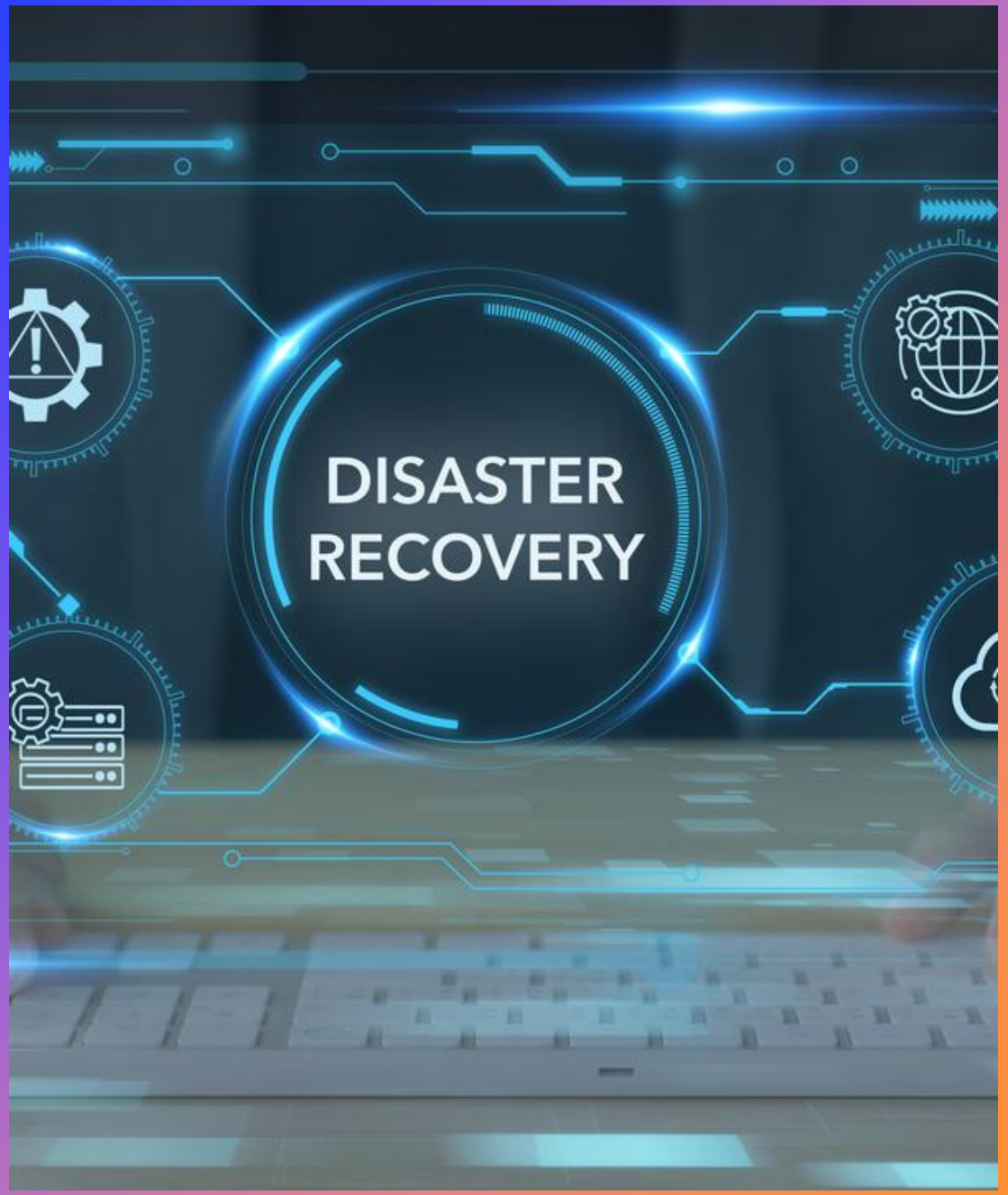
Safely restore business operations and verify normal status.

- ✓ Restore data from clean, verified backups.
- ✓ Test the systems before full operation
- ✓ Monitor closely for reinfection or suspicious behavior.
- ✓ Communicate recovery progress to stakeholders.

LESSONS LEARNED

Turn the incident into long-term organizational strength.

- ✓ Conduct a post-incident review within 7–10 days.
- ✓ Identify what worked, what failed, and why.
- ✓ Update the IR plan, policies, and training materials.
- ✓ Implement technical improvements based on findings.
- ✓ Track metrics: response time, downtime, cost, recovery speed.



Get in touch. We are ready to support!

PATECCO GmbH

+49 (0) 23 23 - 9 87 97 96

www.patecco.com

info@patecco.com